Web Site to Link to For AUP:
http://gradclass.iu12.org/ed526/auprl.htm

The Board of Education approved the revised Policy #815 Acceptable Use of Internet and Network Facilities Policy at the February 15, 2001 meeting. Please review the text of the revised policy printed below. Your building principal will be reviewing this with all staff and students.

Policy #815
ACCEPTABLE USE OF INTERNET AND NETWORK FACILITIES POLICY

1. Purpose / Responsibility

In a free and democratic society, access to information is a fundamental right of citizenship. Electronic information research skills are now fundamental to preparation of citizens and future employees during an age of information. The network is provided for students and staff to conduct research and communicate with others.

The Board supports the use of the Internet and other network facilities in the district's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration.

The use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

The district shall make every effort to ensure that this education resource is used responsibly by students and staff.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

2. Definition

Network facilities refer to computers and peripheral devices connected to the computers.

3. Authority

The electronic information available to students and staff does not imply endorsement of the content by the school district, nor does the district guarantee the accuracy of information received on the Internet.
The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The school district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users.

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator.

Network users take full responsibility for revealing their own personal address or telephone numbers on the network.

4. Guidelines

Users will use this system only for educational and professional or career development activities, and limited, high quality, self-discovery activities.

Network accounts will be used only by the authorized owner of the account for its authorized purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.

System users have a limited privacy expectation in the contents of their personal files on the district system. Routine maintenance and monitoring of the system, including e-mail communications to and from the district, may lead to discovery that the user has or is violating the district acceptable use policy, the discipline policy, or the law.

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files.

No user will connect or disconnect any device from any district or network system without prior approval from the data processing manager or computer coordinator.

On a temporary basis, not to exceed one school year, staff members may bring to school and use computer hardware or software not purchased by the school district provided that such hardware does not require installation by or support from district technology personnel. Any personal equipment remaining beyond one school year will be considered a donation to the school district. Any software not purchased by the school district must be validly licensed to the user.

Should any individual or organization wish to donate technology equipment to the school district, that individual or organization must contact the district technology coordinator before the equipment is brought into the district and set up to be used. Further, once accepted by the school district, the donated equipment becomes property of the school district.
Prohibitions (This is a subsection under the Guidelines section)

Students and staff are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and State law. Specifically, the following uses are prohibited:

1. Use of the network to facilitate illegal activity.

2. Use of the network for commercial or political purposes outside of the designated sections of the network.

3. Use of the network for hate mail, discriminatory remarks, and offensive or inflammatory communication.

4. Unauthorized or illegal installation, distribution, reproduction, modification, or use of copyrighted materials including unauthorized games, programs, files, or other electronic media.

5. Use of the network to access obscene or pornographic material.

6. Use of inappropriate language or profanity on the network.

7. Use of the network to transmit material likely to be offensive or objectionable to recipients.

8. Use of the network to intentionally obtain or modify files, passwords, and data belonging to other users.

9. Impersonation of another user.

10. Use of network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws.

11. Use of the network to disrupt the work of other users.

12. Destruction, modification, or abuse of network hardware and software.

13. Quoting personal communications in a public forum without the original author's prior consent.

14. Employees and students shall not reveal their passwords to another individual.

15. Individual users are not to use a computer that has been logged in under another student's or teacher's name.

16. Revealing personal information related to any users on the system other than by district staff in the performance of assigned duties.

Consequences for Inappropriate Use

The Board establishes that use of the Internet and network facilities is a privilege, not a right. Any user identified as a security risk or having a history of problems with other computer systems may be restricted from access to the network ranging from limited access to complete denial of access. Inappropriate, unauthorized and illegal use or violation of the prohibitions will result in appropriate disciplinary action which could include the cancellation of privileges or notification of the appropriate legal authorities. Inappropriate, unauthorized, and illegal use of violations of the prohibitions by a student may make the student subject to the Code of Student Conduct up to an including expulsion. Offenders may also be subject to criminal prosecution.

The building administrator shall have the authority to determine what is inappropriate use.

The network users shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. This includes, but is not limited to, malicious attempt to harm or destroy data of another user, Internet or other networks and the uploading or creation of computer viruses.

An individual search may be conducted if there is reasonable suspicion that a user has violated the law or the district policies. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation. District employees should be aware that their personal files may be discoverable under state public records laws.